

DD FORM 254 Continuation Sheet

Contract # ID04140199

Contract Expiration : 31 March 2016

Ref 13.: (CONTINUED)

Ref 10.k.(2): Contractor may require access to Focal Point Programs (FPP)/Alternative Compensatory Control Measures (ACCM). The government Focal Point Control Officer (FPPCO) will determine the appropriate ACCM/FPP accesses to information required under this contract. The contractor must comply with designated FPP/ACCM guidance for protection of ACCM information IAW applicable CJCSM 3213.02 series publication and written instruction from the government FPPCO.

Ref 11.a.: Contract performance is for HQ USAFCENT operations on Shaw AFB and forward operating locations. The highest level of security clearance required for this contract is Top Secret. Using activity will provide security classification guidance for the performance of this contract. The government will oversee the handling and storage of classified information in support of this contract. The government will provide storage capability of all classified material required for this contract. All classified information will be returned to the government upon termination of this contract.

Ref 11.f.: Contractor personnel deployed to overseas locations may have access to classified information under the control of U.S. Military, Host Nation Military or Embassy personnel. The storage of classified by contractor employees at any location abroad that is not under U.S. Government control is prohibited.

Ref 11.j.: The contractor will follow host unit OPSEC program guidance. A copy of local guidance will be provided to the contractor.

Ref 14.: (CONTINUED) classified information IAW DoDM 5200.01, Information Security Program: AFI 31-401, Information Security Program Management; AFI 31-601, Industrial Security Program Management, and other directives deemed necessary for the Security Servicing Activity (SSA). See attached Release of SCI Intelligence Information for additional security requirements. Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefings and a final U.S. Government clearance at the appropriate level. The contractor will follow all applicable security related to the protection of SAP information. Baseline guidance includes CJCSI 3120.08 Series, DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), NISPOM Supplement, DoD 5205.11, Joint Air Force-Army-Navy (JAFAN) 6/0, 6/3, 6/9; applicable Program Security Directives (PSDs) and Security Classification Guides (SCGs), and Local Standard Operating Procedures. The PSO will provide a copy of applicable guidance to the contractor.

Ref 15.: (CONTINUED) Both offices are located at 524 Shaw Drive, Shaw AFB, SC 29152. These offices may be reached at DSN 312-965-3462. Contractor personnel files maintained by the SAP ISO are subject to inspection by SAP inspection authorities and periodic ISO self-inspections. Contractors will comply with STO Chief, ISO or inspector requests for relevant information or assistance to complete periodic inspections commensurate with assigned responsibilities. NSA/Q142 will be the Cognizant Security Authority for all IJSTO material and security procedures. AFOSI-PJ will maintain Cognizant Security Authority over all USAF Special Access Program material and security procedures. Defense Security Service retains cognizance only over non-SCI and non-SAP material released to or developed under the contract and held at the contractor's cleared facility.

DD FORM 254 Continuation Sheet

Ref 17f.: USAFCENT/A2S, 524 Shaw Drive, Shaw AFB SC 29152, USAFCENT/A3XT (STO), 524 Shaw Drive, Shaw AFB SC 29152 and 20 FW/IP, 524 Nelson Ave, Shaw AFB SC 29152.

MARIANNE LAWSON, GS-13, DAF
USAFCENT/A2S

JOHN R. MENDER, GS-13, DAF
Chief, Information Protection

DAVIS J. GUDENAU, GS-13, DAF
AFCENT/A3CT (STO)

ATTACHMENT 1
ADDENDUM TO DD FORM 254

Contract Number: TBD
Expiration Date: 16 Feb 2015

Sensitive Compartmented Information (SCI) Security Guidance

E.O. 12333	United States Intelligence Activities (as amended by E.O. 13284 (2003), E.O. 13355 (2004) and E.O. 13470 (2008))
ICD 704	Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information (1 Oct 2008)
ICD 710	Classification and Control Marking System (11 Sep 2009)
DCID 6/1	Security Policy for Sensitive Compartmented Information and Security Policy Manual (1 Mar 95/ updated 4 Nov 2003)
DCID 6/6	Security Controls on the Dissemination of Intelligence Information (11 Jul 01/updated 6 Jun 2003)
DoD 5105.21-M-1	Sensitive Compartmented Information Administrative Security Manual, Volumes 1 thru 3 (19 Oct 2012)
AFI 14-302	Control, Protection, and Dissemination of Sensitive Compartmented Information (18 Jan 94)
AFI 14-303	Release of Intelligence to U.S. Contractors (1 Apr 99)
AFMAN 14-304	The Security Use, and Dissemination of Sensitive Compartmented Security Information (1 May 99)

ATTACHMENT 3
DD FORM 254, FOR OFFICIAL USE ONLY (FOUO) ADDENDUM

ATTACHMENT TO DD FORM 254 FOR CONTRACT NO: ID04140199

CONTRACT EXPIRATION DATE: 31 March 2016

The following procedures will be used to protect FOUO material:

1. HANDLING:

a. Access to FOUO material shall be limited to those employees needing the material to do their jobs. The FOUO marking is assigned to material created by a DoD User Agency. It is not authorized as a substitute for a security classification marking, but is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA). FOUO marking is assigned to information at the time of its creation by a DoD User Agency.

b. Use of the above marking means the information must be reviewed by the Government prior to its release to the public to determine if a significant and legitimate government purpose is served by withholding the information or portions of it.

2. IDENTIFICATION MARKINGS:

a) An unclassified document containing FOUO information will be marked "For Official Use Only" at the bottom of the front cover, the first page, each page containing FOUO information, the back page, and the outside of the back cover. Each paragraph containing FOUO information shall be marked as such.

b) Within a classified document, an individual page that contains FOUO and classified information will be marked at the top and bottom with the highest security classification of information appearing on the page. If an individual portion contains FOUO information, but no classified information, the portion will be marked, "FOUO".

c) If a classified document also contains FOUO material or if the classified material becomes FOUO when declassified, place the following statement on the bottom of the cover or first page under the classification marking: "NOTE: If declassified, review the document to make sure material is not FOUO and not exempt under DoD Regulation 5400.7/AF Supplement before public release".

d) Mark other records such as computer print outs, photographs, films, tapes, or slides "FOR OFFICIAL USE ONLY" so the receiver or viewer knows the record contains FOUO material.

e) Mark each part of a message that contains FOUO material. Unclassified messages containing FOUO material must show the abbreviation "FOUO" before the text begins.

f) Insure documents that transmit FOUO material call attention to any FOUO attachments.

ATTACHMENT 3
DD FORM 254, FOR OFFICIAL USE ONLY (FOUO) ADDENDUM

g) Any FOUO information released to a contractor by a DoD User Agency is required to be marked with the following statement prior to transfer: "This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemptions ____ apply."

h) The originator or other competent authority can only accomplish removal of the FOUO marking. When the FOUO status is terminated, all known holders will be notified to the extent practical.

3. **DISSEMINATION:** Contractors may disseminate FOUO information to their employees and subcontractors who have a need for the information in connection with the management of the contract.

NOTE: FOUO is not automatically linked to a "classified" contract; many non-classified contracts require access to FOUO information.

4. **STORAGE:** During normal duty hours, place FOUO material in an out-of-sight location, if your work area is accessible to persons who do not have a valid need for the material. After normal duty hours, store FOUO material to prevent unauthorized access. File with other unclassified records in unlocked buildings or rooms usually provide adequate after-hours protection. For additional protection, store FOUO material in a locked container such as file cabinets, desks or bookcases. Expenditure of funds for security container or closed areas solely for the protection of FOUO material is prohibited.

5. **TRANSMISSION:** FOUO material shall be transmitted by the same methods as other unclassified material. Discussion of FOUO material on the telephone is authorized if necessary for the performance of the contract. FOUO material may be transmitted over telephone lines in digital form, by telecopies, or by other DSN teletype lines.

6. **RELEASE:** FOUO material shall not be released outside the contractor's facility except to representatives of the DoD. Unauthorized disclosure of FOUO information does not constitute a security violation, but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal actions.

7. **DESTRUCTION:** When no longer needed, FOUO material shall be disposed of by a method that precludes its disclosure to unauthorized individuals and placed in a regular trashcan.

Attachment 2
DD Form 254, Block 14 Continued

**RELEASE OF SCI/NON - SCI INTELLIGENCE INFORMATION
TO DOD CONTRACTORS**

ATTACHMENT TO DD FORM 254 FOR CONTRACT: ID04140199

CONTRACT EXPIRATION DATE: 31 March 2016

**RELEASE OF SENSITIVE COMPARTMENTED INFORMATION (SCI)
INTELLIGENCE INFORMATION TO U.S. DoD CONTRACTORS**

1. Requirements for access to SCI:

a. All SCI will be handled in accordance with special security requirements, which will be furnished by the local Special Security Office (SSO) USAFCENT/A2S or Special Security Representative (SSR). Specific security directives provided by the SSO will be included in Block 13 of the DD Form 254.

b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated Contracting Officer's Representative (COR).

c. Names of contractor personnel requiring access to SCI will be submitted to the COR for approval. (The COR is identified on the reverse side of the DD Form 254 or by COR appointment letter.) Upon receipt of written approval from the COR, the company security officer will submit request(s) for special background investigations in accordance with the NISPOM to the Intelligence Support Office. The entire personnel security questionnaire package should not be forwarded to the Intelligence Support Office. The Contractor Special Security Officer (CSSO) must follow the instructions provided by the Intelligence Support Office to the CSSO.

d. Inquiries pertaining to classification guidance on SCI will be directed through the CSSO to the responsible COR as indicated on the DD Form 254 or by COR appointment letter.

e. SCI furnished in support of this contract remains the property of the Department of Defense (DoD) department, agency, or command originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the COR.

f. SCI will be stored and maintained only in properly accredited facilities at the contractor location.

2. The Contracting Officers Representative (COR) will:

a. Monitor the day-to-day activities of DoD SCI contracts and serve as a technical representative. COR serves as a point of contact for CSSO and USAFCENT/A2S.

b. Review the SCI product for contract applicability and determine that the contractor requires the product to complete contractual obligations.

c. Prepare or review contractor access requests to ensure satisfactory justification (need-to-know) and completeness of required information.

d. Prepare and maintain a current SCI employee roster with an information copy to USAFCENT/A2S

quarterly or when requested by the SSO.

e. Approve and coordinate visits by contractor employees through the local SSO when such visits are conducted as part of the contract effort.

f. Maintain records of all SCI material provided to the contractor in support of the contract effort. By 15 January (annually), provide the contractor, for inventory purposes, with a complete list of all documents transferred by contract number, organizational control number, copy number, and document file.

g. Determine dissemination of SCI studies or materials originated or developed by the contractor.

h. Within 30 days after completion of the contract, provide written disposition instructions for all SCI material furnished to, or generated by, the contractor with an information copy to USAFCENT/A2S.

i. Review and forward all contractor requests to process SCI electronically to the USAFCENT/A2S for coordination through appropriate SCI channels.

j. Request for release of intelligence material to a contractor must be prepared by the COR and submitted to USAFCENT/A2S. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirement and copies of the DD Form 254 and Statement of Work (SOW).

RELEASE OF NON-SENSITIVE COMPARTMENTED INFORMATION (NON-SCI) INTELLIGENCE INFORMATION TO U.S. DoD CONTRACTORS

1. Requirements for access to non-SCI:

a. All intelligence material released to the contractor remains the property of the US Government and may be withdrawn at any time. Contractors must maintain accountability for all classified intelligence released into their custody.

b. The contractor must not reproduce intelligence material without the written permission of the originating agency through the Intelligence Support Office. If permission is granted, each copy shall be controlled in the same manner as the original.

c. The contractor must not destroy any intelligence material without advance approval or as specified by the Contracting Officers Representative (COR).

d. The contractor must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract with a valid need to know. Further dissemination to other contractors, subcontractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the originating agency through the COR.

e. The contractor must ensure each employee having access to intelligence material is fully aware of the special security requirements for this material and shall maintain records in a manner that will permit the contractor to furnish, on demand, the names of individuals who have had access to this material in their custody.

f. Intelligence material must not be released to foreign nationals or immigrant aliens whether they are consultants, US contractors, or employees of the contractor and regardless of the level of their security clearance, except with advance written permission from the originator. Requests for release to foreign nationals shall be initially forwarded to the COR and shall include:

- (1) A copy of the proposed disclosure.

(2) Full justification reflecting the benefits to US interests.

(3) Name, nationality, particulars of clearance, and current access authorization of each proposed foreign national recipient.

g. Upon completion or termination of the classified contract, or sooner when the purpose of the release has been served, the contractor will return all classified intelligence (furnished or generated) to the source from which received unless retention or other disposition instructions (see Air Force Records Disposition Schedule) are authorized in writing by the COR.

h. The contractor must designate an individual who is working on the contract as custodian. The designated custodian shall be responsible for receipting and accounting for all classified intelligence material received under this contract. This does not mean that the custodian must personally sign for all classified material. The inner wrapper of all classified material dispatched should be marked for the attention of a designated custodian and must not be opened by anyone not working directly on the contract.

i. Within 30 days after the final product is received and accepted by the procuring agency, classified intelligence materials released to or generated by the contractor, must be returned to the originating agency through the COR unless written instructions authorizing destruction or retention are issued. Requests to retain material shall be directed to the COR for this contract in writing and must clearly indicate the justification for retention and identity of the specific document to be retained.

j. Classification, regarding, or declassification markings of documentation produced by the contractor shall be consistent with that applied to the information or documentation from which the new document was prepared. If a compilation of information or a complete analysis of a subject appears to require a security classification other than that of the source documentation, the contractor shall assign the tentative security classification and request instructions from the COR. Pending final determination, the material shall be safeguarded as required for its assigned or proposed classification, whichever is higher, until the classification is changed or otherwise verified.

2. Intelligence material carries special markings. The following is a list of the authorized control markings of intelligence material:

a. "Dissemination and Extraction of Information Controlled by Originator (ORCON)." This marking is used, with a security classification, to enable a continuing knowledge and supervision by the originator of the use made of the information involved. This marking may be used on intelligence, which clearly identifies, or would reasonably permit ready identification of an intelligence source or method, which is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may not be used when an item or information will reasonably be protected by use of other markings specified herein, or by the application of the "need-to-know" principle and the safeguarding procedures of the security classification system.

b. "Authorized for Release to (Name of Country(ies)/International Organization." The above is abbreviated "REL ." This marking must be used when it is necessary to identify classified intelligence material the US government originator has predetermined to be releasable or has been released through established foreign disclosure channels to the indicated country(ies) or organization.

3. The following procedures govern the use of control markings.

a. Any recipient desiring to use intelligence in a manner contrary to restrictions established by the control marking set forth above shall obtain the advance permission of the originating agency through the COR. Such permission applies only to the specific purposes agreed to by the originator and does not automatically apply to all recipients. Originators shall ensure that prompt consideration is given to recipients' requests in these regards, with particular attention to reviewing and editing, if necessary, sanitized or

paraphrased versions to derive a text suitable for release subject to lesser or no control markings.

b. The control marking authorized above shall be shown on the title page, front cover, and other applicable pages of documents, incorporated in the text of electrical communications, shown on graphics, and associated (in full or abbreviated form) with data stored or processed in automatic data processing systems. The control marking also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions. If the control marking applies to several or all portions, the document must be marked with a statement to this effect rather than marking each portion individually.

c. The control markings shall be individually assigned at the time of preparation of intelligence products and used in conjunction with security classifications and other marking specified by E.O. 12958 and its implementing security directives. The marking shall be carried forward to any new format in which the same information is incorporated including oral and visual presentations.

4. Request for release of intelligence material to a contractor must be prepared by the COR and submitted to the USAFCENT/A2S. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirements and copies of the DD Form 254 and Statement of Work (SOW).